AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1-15. (Canceled)

16. (New) A method of securing access to a piece of equipment, the method comprising:

creating a reference datum for an authorized user, in an authentication medium, wherein said reference datum comprises at least an encrypted authentic biometric signature;

storing said encrypted authentic biometric signature on a computer associated with said piece of equipment;

acquiring, at a sensor, a plain biometric signature for a user requesting access to said piece of equipment;

decrypting, in said authentication medium, said encrypted authentic biometric signature stored on said computer;

verifying, in said authentication medium, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of an authorized user; and

granting said user access to said piece of equipment if said comparison is successful and denying access if said comparison fails.

17.   (New) The method according to claim 16, wherein said authentication medium is an electronic card.

18.   (New) The method according to claim 17, wherein said electronic card includes a decryption module.

19.   (New) The method according to claim 17, wherein said electronic card includes a comparison module, and said comparing is performed in said electronic card.

20.   (New) The method according to claim 17, wherein said electronic card further comprises an encryption module.

21.   (New) A method of securing access to a piece of equipment, the method comprising:

creating a reference datum for an authorized user in an authentication medium, wherein the creation of said reference datum comprises:

(i)   inputting a personal identification code for said authorized user on a keyboard;

(ii)   detecting, at a sensor, a plain authentic biometric signature for said authorized user;

(iii)   encrypting said plain authentic biometric signature by means of a private key;

    (iv)   sending said encrypted authentic biometric signature to a computer associated with said piece of equipment;

    (v)   associating said personal identification code with said encrypted authentic biometric signature; and

    (vi)   storing said encrypted authentic biometric signature and said associated personal identification code on said computer;

receiving a personal identification code inputted on a keyboard;

acquiring, at a sensor, a plain biometric signature of a user requesting access to said piece of equipment; and

verifying the authenticity of said plain biometric signature for a user requesting access to said piece of equipment, wherein said verifying comprises:

    (i)   matching said personal identification code with an encrypted authentic biometric signature stored on said computer;

    (ii)   sending said encrypted authentic biometric signature, that is associated with said personal identification code, to said authentication medium;

    (iii)   decrypting said authentic biometric signature, on said authentication medium, by means of a secret key on said authentication medium;

    (iv)   comparing, on said authentication medium, said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result; and

(v)   granting access to said user requesting access to said piece of

equipment if said comparison result is successful and denying

access if said comparison result fails.

22.   (New) The method according to claim 21, wherein said authentication

medium is an electronic card.

23.   (New) The method according to claim 22, wherein said electronic card

includes a decryption module.

24.   (New) The method according to claim 22, wherein said electronic card

includes a comparison module, and said comparing step is performed in said

electronic card.

25.   (New) The method according to claim 22, wherein said electronic card

includes an encryption module.

26.   (New)   A device for securing access to a piece of equipment,

comprising:

        at least one computer, associated with said piece of equipment, for storing

an encrypted authentic biometric signature and a corresponding personal

identification code of an authorized user;

        a sensor for acquiring a plain biometric signature of a user requesting access

to said piece of equipment; and

an authentication medium having a controller, wherein said controller:

receives said encrypted authentic biometric signature, associated with said personal identification code;

decrypts said authentic biometric signature by means of a secret key;

compares said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result; and

grants access to said user requesting access to said piece of equipment if said comparison is successful and denying access if said comparison fails.

27.   (New) The device according to claim 26, further comprising:

at least one computer for storing a plurality of encrypted authentic biometric signatures and a corresponding plurality of personal identification codes for a corresponding plurality of authorized users, wherein said at least one computer:

delivers an encrypted authentic biometric signature associated with a personal identification code to said authentication medium when receiving an access request from a user, such that said authentication medium is capable of providing a plurality of users secure access to said piece of equipment.

28.   (New) The device according to claim 26, wherein said authentication medium is an electronic card having a memory storing a secret key that cannot be read from outside.

29. (New) The device according to claim 26, further comprising an encryption module that encrypts an authentic biometric signature supplied in plain form to said sensor and delivers said encrypted authentic biometric signature to said at least one computer, in response to an encryption command.

30. (New) The device according to claim 29, wherein said secret key is a private key having a matching public key, and wherein said encryption module is included in said at least one computer and uses said matching public key.